UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/392,938	09/09/1999	ROBERT B. TACKMAN	99-1852	2037

24938 7590 01/12/2005

DAIMLERCHRYSLER INTELLECTUAL CAPITAL CORPORATION
CIMS 483-02-19
800 CHRYSLER DR EAST
AUBURN HILLS, MI 48326-2757

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/392,938	TACKMAN ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cov r sheet with the correspondenc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 September 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment filed July 20, 2004 has been carefully considered; however, the cited reference, Rowney (US 5,987,140), does not clearly and explicitly state the use and process of electronic agreement, electronic document, or electronic chattel paper document. Therefore the new ground(s) of rejection is presented in this Office action.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney (US 5,987,140), and further in view of Ginter et al (US 5,892,900).

a. *Referring to claim 1:*

i. Rowney teaches:

(1) a server processing unit and a server memory device electrically coupled to the server processing unit **[i.e., a workstation having a central processing unit, such as a microprocessor, and a number of other units (including a Random Access Memory (RAM) and Read Only Memory(ROM)) interconnected via a system bus (column 4, line 1-10)]**,

(2) a client processing unit and a client memory device electrically coupled to the client processing unit **[i.e., a personal computer having a central processing unit, such as a microprocessor, and a number of other units (including a Random Access Memory (RAM) and Read Only Memory(ROM)) interconnected via a system bus (column 4, line 1-10)]**,

(3) a server program module, stored in the server memory device, for providing instructions to the server processing unit **[i.e., the**

workstation typically has installed an operating system such as the IBM OS/2 operating system or UNIX operating system (column 4, line 15-20)],

(4) a client program module, stored in the client memory device, for providing instructions to the client processing unit **[i.e., the personal computer includes an operating system such as the Microsoft Windows Operating System (OS) (column 4, 15-17)],** and

(5) a communication medium, communicatively coupling the server processing unit and the client processing unit **[i.e., secure transmission of data is provided between a plurality of computer systems over a public communication systems, such as the Internet (column 2, line 60-62)];**

(6) the client processing unit, responsive to the instruction of the client program module and the server processing unit, responsive to the instructions of the server program module **[figure 2]**, being operative to:

(a) authorize access to the system **[i.e., customer computer system transmits a client certificate to enable customer computer system to authenticate the identity of customer computer system (column 11, line 30-34)];**

(b) generate at least one unexecuted electronic chattel paper document **[i.e., customer computer system initiates communication by sending "client hello" message, that is "one unexecuted electronic chattel paper document", to the merchant computer system (column 10, line 31-33)];**

(c) prevent the creation of fraudulent versions of the electronic chattel paper document **[i.e., by using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications between the two computer systems, which may thereafter engage in secure communications with less risk of interception by third parties (column 11, line 53-58)];**

(d) allow signatures electrically input by parties to a chattel paper transaction to be associated with the electronic chattel paper document thereby generating an electronic chattel paper agreement **[i.e., Merchant**

computer system 130 calculates a digital signature 525 for the combined contents of the combined block 530 comprising basic authorization r quest 510, the encryption public key certificate 515 and the signature public key certificate 520, and appends it to the combination of the combined basic authorization request 510, the encryption public key certificate 515 and the signature public key certificate 520. The merchant computer system calculates digital signature 525 by first calculating a "message digest" based upon the contents of the combined basic authorization request 510, the encryption public key certificate 515 and the signature public key certificate 520. A message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. Message digests help verify that a message has not been altered because altering the message would change the digest. The message digest is then encrypted using the merchant computer system's 130 digital signature private key, thus forming a digital signature, that is "generating an electronic chattel paper agreement" (column 12, line 46-65)]; and

(e) maintain an authoritative copy of the electronic chattel paper document in the server memory device of the server processing unit **[i.e., merchant computer system stores capture response for later use in by legacy system accounting program, e.g. to perform reconciliation between the merchant operating merchant computer system and the financial institution from whom payment was requested, thereby completing the transaction (column 20, line 3-8)]**.

ii. Although Rowney does not clearly and explicitly state the use and process of electronic agreement, electronic document, or electronic chattel paper document, Ginter teaches:

(1) Ginter's invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community

members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway. Furthermore, Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce--that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties **(column 2, lines 20-56).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure transaction management and to ensure that information is accessed and/or otherwise used only in authorized ways, and maintains the integrity, availability, and/or confidentiality of such information and processes related to such use **(column 1, lines 9-15 of Ginter).**

iv. The ordinary skilled person would have been motivated to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure chains of handling and control for both information content and information employed to regulate the use of such content and consequences of such use. It also relates to systems and techniques that manage, including meter and/or limit and/or otherwise monitor use of electronically stored and/or disseminated information **(column 1, lines 20-30 of Ginter).**

b. *Referring to claim 2:*

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving access information from the input device **[i.e., server certificate enables customer computer system to authenticate the identity of merchant computer system (column 11, line 14-17)]**,

(b) transmitting the access information to the server over the communication medium **[i.e., customer computer system transmits client certificate to the merchant computer system enabling the server to authenticate the identity of customer computer system (column 11, line 30-34)]**, and

(c) receiving an authorization indicator from the server processing unit over the communication medium **[i.e., server hello message includes an indicator of the cryptographic algorithms selected from among the algorithms specified by client hello message, which will be used in further encrypted communications (column 11, line 10-13)]**; and

(3) the server processing unit **[i.e., Figure 1A]**

(a) receiving the access information from the client processing unit over the communications medium **[i.e., message communicated by customer computer system to merchant computer system may be of goods and services to be ordered and payment information(column 11, line 59-64)]**,

(b) verifying that the access information qualifies for granting access to the system **[i.e., merchant computer system processes the purchase request from customer in accordance with the authorization response, determining whether a request should be granted or denied (column 16, line 13-20)]**, and

(c) transmitting an authorized indicator to the client processing unit over the communication medium **[i.e., server hello message includes an indicator of the cryptographic algorithms selected from among the algorithms specified by client hello message, which will be used in further encrypted communications (column 11, line 10-13)]**;

c. *Referring to claim 3:*

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving pertinent information from the input **[i.e., server hello message allowing client to connect with merchant computer system (column 10, line 61-62)]**, and

(b) integrating the pertinent information into an electronic template **[i.e., combining the server hello message and client related message sent by customer computer system or client wherein the message that specify goods or services to be ordered and payment information (column 11, line 59-63)]**;.

d. *Referring to claim 4:*

i. Rowney further teaches:

(1) receiving a complete indicator from the input device, the complete indicator indicating that no additional pertinent information will be received by the client processing unit **[i.e., merchant computer system provides server certificate or server key exchange message and as well as server hello done message (column 11, line 25-28)]**, and

(2) merging the pertinent information and the predefined document information to generate the electronic chattel paper document conforming to the predefined chattel paper document format **[i.e., combining the server message and client related message sent by customer computer system or client wherein the message that specify goods or services to be ordered and payment information (column 11, line 59-63)]**;

e. *Referring to claim 5:*

i. Rowney further teaches:

(1) an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic chattel paper document by the client processing unit, in response to generating the electronic chattel paper document, rejecting any attempts to modify the electronic document **[i.e.,**

payment gateway computer system verifies merchant computer system's encryption and signature public key certificates by calculating a m ssage over the content of said combined authorization request, then decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system. If the two messages are the same, the digital signature is validated, otherwise, payment gateway computer system rejects the authorization request (column 14, line 4-14)].

f. *Referring to claim 6:*

i. Rowney further teaches:

(1) an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic document by the client processing unit, in response to generating the chattel paper electronic document, encrypting the electronic chattel paper document and generating a signature key based at least in part on the contents of the electronic chattel paper document **[i.e., the merchant computer systems combines basic authorization request, a copy of its encryption public key certificate, and a copy of its signature public key certificate. It further calculates a digital signature for the combined contents/messages of the combine block comprising basic authorization request. The merchant computer system calculates digital signature by first calculating a "message digest" based upon the contents of the combined basic authorization request. Message digest help verify that a message has not been altered because altering the message would change the digest. The message digest is then encrypted using the merchant computer system's digital signature private key (column 12, line 43-65)].**

g. *Referring to claim 7:*

i. Rowney further teaches:

(1) the client processing unit **[i.e. Figure 1A]**

(a) in response to generating the electronic document, encrypting the electronic document **[i.e., the message digest is then**

encrypted using the merchant computer system's digital signature private key (column 12, line 63-65)], and

(b) in response to an attempt to modify the electronic chattel paper document, rendering the electronic chattel paper document invalid **[i.e., a message digest help verify that a message has not been altered because altering the message would change the digest (column 12, line 60-63), and payment gateway computer system verifies merchant computer system's encryption and signature public key certificates by calculating a message over the content of said combined authorization request, then decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system. If the two messages are the same, the digital signature is validated, otherwise, payment gateway computer system rejects the authorization request (column 14, line 4-14)].**

h. *Referring to claim 8:*

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving at least one signature input from the input device **[i.e., payment gateway computer system receives and verifies merchant computer system's encryption and signature public key certificates, and as well as digital signature (column 13, line 54-58)],**

(b) creating a signature file containing the signature input **[i.e., payment gateway computer system creates a basic authorization response, and a copy of its signature public key certificate (column 14, line 25-35)]** , and

(c) encrypting the signature file using an encryption key that is based at least in part on the contents of the electronic chattel paper document **[i.e., payment computer system calculates a digital signature by first calculating a message digest based on the contents of the combined basic authorization response and the signature public key certificate. The message**

digest is then encrypted using the merchant computer system's digital signature private key (column 14, line 40-50)].

i. *Referring to claim 9:*

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving a submit indicator from the input device **[i.e., in order to obtain payment from the customer, the merchant must supply/submit payment information to the bank or other payment gateway responsible for the payment method (column 11, line 65-68)]**, and

(b) in response to receiving the submit indicator, transmitting the electronic chattel paper document and the electronically input signatures associated with the electronic chattel paper agreement to the server processing unit over the communication medium **[i.e., the merchant computer systems transmits a payment authorization request by combining basic authorization request, a copy of its encryption public key certificate, and a copy of its signature public key certificate. It further calculates a digital signature for the combined contents/messages of the combined block comprising basic authorization request, then transmits over the communication network (column 12, line 43-53)]**; and

(2) the server processing unit **[i.e., Figure 1A]**

(a) receiving the electronic chattel paper agreement and the electronically input signatures **[i.e., payment gateway computer system receives a payment authorization request and verifies merchant computer system's encryption and signature public key certificates, and as well as digital signature (column 13, line 54-58)]**,

(b) preventing any modifications to the electronic chattel paper agreement and the signature file **[i.e., then decrypting digital signature to obtain a copy of the exact message, that is "preventing any modifications to the electronic chattel paper agreement and the signature file", calculated by the merchant computer system. If the two messages are the sam , the digital**

signature is validated, otherwise, payment gateway computer system rejects the authorization request (column 14, line 4-14)], and

(c) providing an unauthorized copy indicator on any electronic and hard copies of the electronic chattel paper agreement, the unauthorized copy indicator indicating that the electronic and hard copies of the electronic chattel paper agreement are not the authoritative copy of the electronic chattel paper agreement **[i.e., payment gateway computer system contacts the appropriate financial institution using a secure means, e.g., a direct-dial modem-to-modem connection, or a proprietary internal network that is not accessible to third parties, and using prior art means, obtains a response indicating whether the requested payment is authorized (column 14, line 16-24)].**

j. *Referring to claim 10:*

i. Rowney teaches:

(1) receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic chattel paper document **[i.e., payment gateway system receives and processes a payment authorization request from the merchant (column 12, line 15-20];**

(2) in response to receiving a complete indicator from the input source, the complete indicator indicating that the received subset of input information is complete, generating an electronic chattel paper document by merging the subset of input information with a chattel paper document template **[i.e., the gateway system then generates the basic authorization response and combines it with a copy of its signature public key certificate. The data request is then encrypted using the merchant computer system's digital signature private key and transmits it back to the merchant computer system (column 14, line 25-50)];**

(3) electronically receiving a set of signatures by parties to a chattel paper transaction from the input source, whereby up receiving the set of chattel paper signatures, the electronic chattel paper document is considered an

electronic chattel paper agreement **[i.e., the merchant computer system then decrypts digital signatur to obtain a copy of the equivalent data request. If the two data requests are the same, the digital signature (that is "an electronic chattel paper agreement") is validated (column 16, line 3-8)]**; and

(4) in response to receiving a submit indicator, storing the electronic chattel paper agreement within an access restricted computer system, the stored electronic chattel paper agreement constituting an authoritative copy of the electronic chattel paper agreement **[i.e., the merchant computer system stores capture response for later use in by legacy system accounting program, in which to perform reconciliation between the merchant and the financial institution, thereby completing the transaction (colulmn 20, line 3-8)].**

ii. Although Rowney does not clearly and explicitly state the use and process of electronic agreement, electronic document, or electronic chattel paper document, Ginter teaches:

(1) Ginter's invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway. Furthermore, Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce--that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties **(column 2, lines 20-56).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure transaction management and to ensure that information is accessed and/or otherwise used only in authorized ways, and maintains the integrity, availability, and/or confidentiality of such information and processes related to such use **(column 1, lines 9-15 of Ginter).**

iv. The ordinary skilled person would have been motivated to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure chains of handling and control for both information content and information employed to regulate the use of such content and consequences of such use. It also relates to systems and techniques that manage, including meter and/or limit and/or otherwise monitor use of electronically stored and/or disseminated information **(column 1, lines 20-30 of Ginter).**

k. *Referring to claim 11:*

i. Rowney further teaches:

(1) after the generating the electronic chattel paper document providing a signature indicator to the input source, the signature indicator indicating that the generating step is complete and that the electronic documents requires the input of the set of electronic signatures **[i.e., payment gateway computer system validates merchant digital signature, that is "the electronic chattel paper document" (column 14, line 1-2)].**

l. *Referring to claim 12:*

i. Rowney further teaches:

(1) encrypting the electronic chattel paper document **[i.e., the payment gateway computer system calculates digital signature (that is "the electronic chattel paper document") by first calculating a message digest based on the contents of the combined basic authorization response and signature**

public key certificate. The message digest is then encrypted using the merchant computer system's digital signature private key (column 14, line 25-50)];

m. *Referring to claim 13:*

i. Rowney further teaches:

(1) preventing the electronic document from being modified **[i.e., the payment gateway computer system uses a message digest method to detect if the contents have been altered. The message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. It helps verify that a message has not been altered because altering the message would change the digest (column 12, line 55-65)].**

n. *Referring to claim 14:*

i. Rowney further teaches:

(1) prior to the storing step,

(a) encrypting the set of electronically input signatures using an encryption key **[i.e., payment gateway computer system encrypts combined block using random encryption key RK-1 to form encrypted combined block. It then encrypts random encryption key RK-1 using the public key of merchant computer system to form encrypted random key RK (column 14, line 56-68)],**

(b) the encryption key being based, at least in part, on the contents of the electronic chattel paper document **[i.e., the payment gateway computer system calculates digital signature by first calculating a message digest based on the contents of the combined basic authorization response and signature public key certificate. The message digest is then encrypted using the merchant computer system's digital signature private key (column 14, line 25-50)],** whereby

(c) if the contents of the electronic chattel paper document are modified, the electronically input signatures and the electronic chattel paper agreement will be invalid **[i.e., after decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system, if the**

two messages are the sam , th digital signature is validated. Otherwise, payment gateway computer system rej cts the authorization request, and the electronic agreement is counterfeit (column 14, line 4-14)].

o. *Referring to claim 15:*

i. Rowney further teaches:

(1) providing an indicator that the set of electronically input signatures has been received and that the electronic chattel paper agreement is complete **[i.e., payment gateway computer system receives a payment authorization request and verifies merchant computer system's encryption and signature public key certificates, and as well as digital signature (column 13, line 54-58)].**

p. *Referring to claim 16:*

i. Rowney teaches:

(1) a client device receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic chattel paper document and a set of signatures necessary to make the electronic chattel paper document a binding chattel paper agreement **[i.e., payment gateway computer system receives and processes a payment authorization request from the merchant, where the authorization request combines with a copy of its encryption public key certificates and a copy of its signature public key certificate (column 12, line 15-20 and line 43-48)];**

(2) a client device encrypting the electronic chattel paper document using a first key and the set of signatures using a second key, the second key being based at least in part on the contents of the electronic chattel paper document, whereby any modifications to the electronic document would result in invalidating the set of signatures **[i.e., the payment gateway computer system uses its private key to encrypted random key contained within received merchant authorization request, thereby decrypting it and obtaining a cleartext version of random key RK-0, the gateway system then applies random key RK-0 to encrypted combined block, thereby decrypting it and obtaining a cleartext version of combined block.**

Finally, the gateway system decrypts digital signatur to obtain a copy of the equivalent data requ st. If the two data requests are the same, the digital signature is validated. If the validation fails, the gateway computer system rejects the authorization request (column 13, line 45-53; and column 14, line 8-14)];

(3) a client device transferring the encrypted electronic chattel paper document and the encrypted set of signature to a server device over a communication medium, the server device being access restricted, the stored electronic chattel paper document and set of signature constituting the only authoritative copy of the electronic chattel paper agreement **[i.e., the merchant computer system stores capture response for later use in by legacy system accounting program, in which to perform reconciliation between the merchant and the financial institution, thereby completing the transaction (colulmn 20, line 3-8)].**

ii. Although Rowney does not clearly and explicitly state the use and process of electronic agreement, electronic document, or electronic chattel paper document, Ginter teaches:

(1) Ginter's invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway. Furthermore, Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce--that is commercial relationships regarding products and services can be

shaped through the negotiation of one or more agreements between a variety of parties **(column 2, lines 20-56).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure transaction management and to ensure that information is accessed and/or otherwise used only in authorized ways, and maintains the integrity, availability, and/or confidentiality of such information and processes related to such use **(column 1, lines 9-15 of Ginter).**

iv. The ordinary skilled person would have been motivated to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure chains of handling and control for both information content and information employed to regulate the use of such content and consequences of such use. It also relates to systems and techniques that manage, including meter and/or limit and/or otherwise monitor use of electronically stored and/or disseminated information **(column 1, lines 20-30 of Ginter).**

q. *Referring to claim 17:*

i. Rowney teaches:

(1) a client processing uint **[i.e., Figure 1A];**

(2) a client memory device **[i.e., Figure 1A, a Random Access Memory (RAM) 14 and Read Only Memory (ROM) 16],**

(a) a display device **[i.e., Figure 1A, display device (38)]** and

(b) an input device **[i.e., Figure 1A, a keyboard (24), a microphone (32), a mouse (26), and a speaker (28)]**

(3) a client program module, stored in the client memory, for proving instructions to the client processing unit **[i.e., the personal computer or workstation typically has resident an operating system such as the Microsoft Windows Operating System(OS), the IBM OS/2 operating system, etc.. (column 4, line 14-16)]**;

(4) a communication medium, communicatively coupling the client system to the electronic document system **[i.e., Figure 1A, communication adapter (34) for connecting the personal computer or workstation to a communication network, which operates with a secure communication protocol such as the SSL protocol (column 4, line 10-13 and column 10, line 7-8)]**

(5) the client processing unit **[i.e., Figure 1A]**, responsive to the instructions of the client program module, being operative to:

(6) authorize access to the electronic chattel paper document system by **[i.e., customer computer system transmits a client certificate to enable merchant computer system to authenticate the identity of customer computer system (column 11, line 30-34)]**

(a) receiving access information from the input device **[i.e., server certificate enables customer computer system to authenticate the identity of merchant computer system (column 11, line 14-17)]**,

(b) transmitting the access information to the server over the communication medium **[i.e., customer computer system transmit client certificate to the merchant computer system enabling the server to authenticate the identity of customer computer system (column 11, line 30-34)]**, and

(c) receiving an authorization indicator from the server processing unit over the communication medium **[i.e., server hello message**

includes an indicator of th cryptographic algorithms selected from among the algorithms specified by client hello message, which will be used in furth r encrypted communications (column 11, line 10-13)];

(7) generate at least one electronic chattel paper document **[i.e., customer computer system initiates communication by sending "client hello" message to the merchant computer system (column 10, line 31-33)];**

(8) prevent the creation of fraudulent versions of the electronic chattel paper document **[i.e., by using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications between the two computer systems, which may thereafter engage in secure communications with less risk of interception by third parties (column 11, line 53-58)];**

(9) allow electronically input signatures to be associated with the electronic chattel paper document thereby generating an electronic chattel paper agreement **[i.e., receiving a server key exchange message, which may be used by a client to decrypt further message sent by the server (column 11, line 20-24)]**,

(a) receiving a set of signatures from the input device **[i.e., receiving a server key exchange message, which may be used by a client to decrypt further message sent by the server (column 11, line 20-24)]**

(b) creating at least one signature file containing the set of signature **[i.e., establishing a client key exchange message which may be used by the server to decrypt message sent by the client (column 11, line 40-44)]** , and

(c) encrypting the signature using a encryption key that is based at least in part on the contents of the electronic chattel paper document

[i.e., using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications b twe n the two computer systems (column 11, line 53-55)]; and

(10) transfer the electronic chattel paper document and the encrypted signature file as an electronic chattel paper agreement to the server over the communication medium **[i.e., client transmit a complete message to the server by including a set of encryption keys, which may thereafter engage in secure communications with less risk of interception by third parties (column 11, line 45-58)]**;

ii. Although Rowney does not clearly and explicitly state the use and process of electronic agreement, electronic document, or electronic chattel paper document, Ginter teaches:

(1) Ginter's invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway. Furthermore, Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce--that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties **(column 2, lines 20-56).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure transaction management and to ensure that information is accessed and/or otherwise used only in authorized ways, and maintains the integrity, availability, and/or confidentiality of such information and processes related to such use **(column 1, lines 9-15 of Ginter).**

iv. The ordinary skilled person would have been motivated to:

(1) clearly state and/or include the use and process of electronic agreement, electronic document, or electronic chattel paper document in Figure 2 of Rowney's invention to secure chains of handling and control for both information content and information employed to regulate the use of such content and consequences of such use. It also relates to systems and techniques that manage, including meter and/or limit and/or otherwise monitor use of electronically stored and/or disseminated information **(column 1, lines 20-30 of Ginter).**

r. *Referring to claim 18:*

i. Rowney further teaches:

(1) receiving pertinent information from the input device **[i.e., server hello message allowing client to connect with merchant computer system (column 10, line 61-62)],**; and

(2) merging the pertinent information with predefined chattel paper document information to generate an electronic chattel paper document conforming to a predefined chattel paper document format **[i.e., combining the server message and client hello message sent by customer computer system or client wherein the message that specify goods or services to be ordered and payment information (column 11, line 59-63)].**

s. *Referring to claim 19:*

i. Rowney further teaches:

(1) the client processing unit is operative to prevent the creation of fraudulent versions of the electronic chattel paper document by, after generating the electronic chattel paper document, encrypting the electronic chattel paper document and rejecting any attempts to enter additional pertinent information **[i.e., the payment gateway computer system uses a message digest method to detect if the contents have been altered. The message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. It helps verify that a message has not been altered because altering the message would change the digest. The message digest is then encrypted using the merchant computer system's digital signature private key (column 12, line 55-65)].**

t. *Referring to claim 20:*

i. Rowney further teaches:

(1) detecting an attempt to modify the electronic chattel paper document **[i.e., the payment gateway computer system uses a message digest method to detect if the contents have been altered. The message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. It helps verify that a message has not been altered because altering the message would change the digest (column 12, line 55-63)**, and

(2) in response to detecting an attempt, rendering the electronic chattel paper document invalid **[i.e., after decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system, if the two messages are the same, the digital signature is validated. Otherwise, payment gateway computer system rejects the authorization request, and the electronic document is counterfeit (column 14, line 4-14)].**

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Conklin et al (US 6, 141, 653) discloses a multivariate negotiations engine for iterative bargaining which: enables a sponsor to create and administer a community between participants such as buyers and sellers having similar interests; allows a buyer/participant to search and evaluate seller information, propose and negotiate orders and counteroffers that include all desired terms, request sample quantities, and track activity; allows a seller/participant to use remote authoring templates to create a complete Website for immediate integration and activation in the community, to evaluate proposed buyer orders and counteroffers, and to negotiate multiple variables such as prices, terms, conditions etc., iteratively with a buyer (see abstract).

b. Hardy et al (US 6,073,242) discloses An electronic communication authority server that provides centralized key management, implementation of role-based enterprise policies and workflow and projection of corporate authorities over trusted networks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
December 28, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100